Entre normes et réalité: l'ONU et le cyberespace

Après l'invasion de l'Ukraine par la Russie, les discussions sur les cybernormes au sein de l'ONU sont dans l'impasse. Les tensions entre les États-Unis et la Russie empêchent toute avancée significative, en particulier sur les questions de cyberconduite lors d'un conflit armé. Le maintien des groupes de travail de l'ONU et le développement d'espaces de discussion sur les normes au-delà de ce cadre constituent toutefois un signal modeste, mais positif pour l'avenir.

Par Taylor Grossman

Dans les années 1980 et 1990, l'expansion mondiale des technologies de l'information et de la communication (TIC) a placé les gouvernements face à de nouvelles questions réglementaires fondamentales: comment gérer les aspects de ce domaine liés à la défense et à la souveraineté nationales, aux activités criminelles et aux autres prérogatives essentielles des États? Les premières années, il n'existait aucun accord régissant l'application du droit international au cyberespace. Beaucoup de pionniers d'Internet ont tenté d'éviter l'ingérence des États. C'est ainsi que John Perry Barlow, défenseur d'un Internet libertaire, a rédigé en 1996 en Suisse la Déclaration d'indépendance du cyberespace. D'autres ont commencé à s'interroger sur la nécessité de mettre au point un tout nouvel ensemble de normes de comportement dans le cyberespace (voir le rapport du CSS «One, Two, or Two Hundred Internets?»).

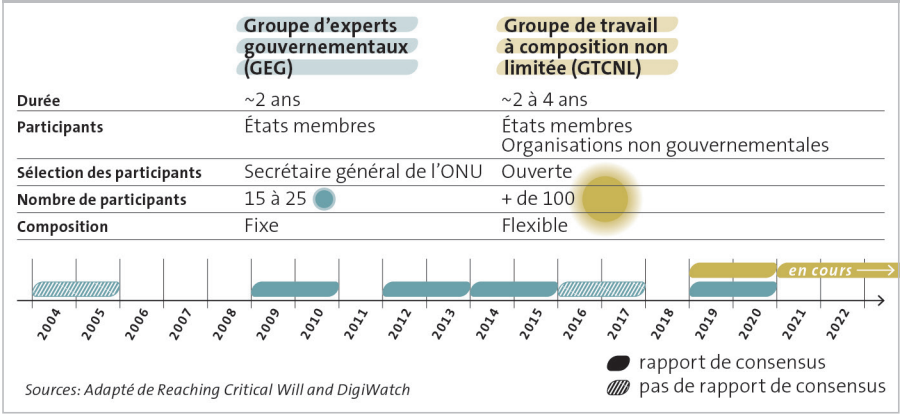
Portrait d'un drapeau de l'ONU sur une carte-mère d'ordinateur, octobre 2022. *Conçu par Kevin Kohler et généré par DALL-E OpenAI*

Dans ce contexte d'incertitude, l'ONU est devenue un point de convergence majeur pour l'élaboration de cybernormes. Ces deux dernières décennies, l'ONU a contribué à faire entrer les TIC dans les lois et normes internationales existantes, y compris sa charte fondatrice, et a établi une certaine continuité afin de garantir le comportement responsable des États dans tous les domaines, en intégrant le cyberespace dans les législations qui réglementent les interactions des États en mer, sur terre et dans les airs. L'ONU s'est notamment efforcée de trouver des normes minimales communes visant à réduire le risque que le cyberespace devienne une source d'instabilité, d'escalade et de dommages – en particulier pour les civils. La Suisse a joué un rôle central dans ces efforts en choisissant de faire de Genève la «capitale de la gouvernance

numérique», en assurant la présidence des précédents cycles de discussion de l'ONU sur les normes et en s'intéressant aux questions de neutralité dans le cyberespace (voir le rapport du CSS «The Law of Neutrality in Cyberspace»).

Pourtant, malgré ce point de départ ambitieux, les deux processus de l'ONU qui en ont découlé – les six groupes d'experts gouvernementaux (GEG) réunis entre 2004 et 2021 et les deux groupes de travail à composition non limitée (GTCNL) mis en place depuis 2019 – ont abouti à des résultats modestes et guindés. De façon générale, les grandes puissances telles que la Russie, la Chine et les États-Unis ont évité l'élaboration de cybernormes détaillées. Si la Chine a parfois coopéré avec d'autres délégations nationales pour faire valoir ses points de vue, la Russie a occupé une place essentielle dans les deux processus de l'ONU – bien que souvent dans le rôle de trouble-fête. À ce jour, les États se sont entendus sur l'applicabilité générale du droit international au cyberespace, mais la plupart n'ont pas encore pris position sur les aspects juridiques plus spécifiques. Et s'agissant du droit international humanitaire (DIH), également appelé «droit des conflits armés», le consensus est encore plus faible. À part une allusion générale à sa pertinence potentielle dans le rapport de consensus du GEG de 2021, les discussions au sein de l'ONU n'ont pas abouti au développement de nouvelles interprétations pratiques. De leur côté, les acteurs non étatiques tentent de se faire davantage entendre dans le discours sur les normes et plaident souvent pour une restriction normative plus rigoureuse du comportement des États.

Aperçu des processus de normes de l'ONU



Sources: Adapté de Reaching Critical Will and DigiWatch

La guerre de la Russie en Ukraine a encore fragilisé les forums de discussion de l'ONU fondés sur le consensus, comme en témoignent les récents blocages de procédure et de fond lors du dernier cycle de réunions du groupe de travail à New York. Les sessions de fond du GTCNL sur la sécurité des TIC et de leur utilisation organisées ce printemps et cet été ont certes débouché sur un rapport d'activité consensuel, mais qui ne contient aucun progrès concret. Ces résultats bien ternes soulignent le divorce croissant entre les discussions sur les normes et les réalités de la politique interétatique, ces plateformes ayant très peu œuvré pour répondre à la situation actuelle en Ukraine. En fin de compte, le principal intérêt de ce groupe de travail est son maintien comme point de contact pour garantir le dialogue et favoriser la mise en place d'autres voies de mise en œuvre des normes. La Suisse plaide toujours pour un processus solide reposant sur l'ONU et a contribué à élargir la liste des participants au groupe de travail, ce qui a ouvert de nouveaux espaces prometteurs au-delà du cadre de l'ONU.

> Il existe un divorce croissant entre les discussions sur les normes et les réalités de la politique interétatique.

Histoire de deux processus

En 1998, la délégation russe auprès de l'ONU a proposé d'intégrer à l'ordre du jour provisoire un point sur les TIC, invoquant les effets néfastes que ces nouvelles technologies pourraient avoir sur la stabilité internationale et la sécurité des États. La Première Commission de l'ONU sur les questions de désarmement et de sécurité internationale a alors créé un groupe d'experts gouvernementaux (GEG) pour se pencher sur le sujet. Ce mécanisme désormais répandu offre une plateforme concrète pour explorer de nouveaux domaines en réunissant des spécialistes qui examinent et recommandent des mesures sans enfermer les États dans des résolutions contraignantes. Six GEG ont ainsi été convoqués entre 2004 et 2021, avec un succès mitigé. Si le premier GEG n'a pas réussi à produire un rapport de consensus, les suivants ont pu prendre de timides mesures. Mais surtout, le rapport du GEG de 2013 a affirmé l'applicabilité du droit international à l'utilisation des TIC par les États et le rapport de 2015 a défini onze normes volontaires de comportement des États. Dotés de mandats restreints, ces GEG se sont concentrés sur les questions politiques et militaires, plutôt que sur les aspects techniques des cybertechnologies. Par exemple, le rapport de 2015 propose une norme prévoyant que les États s'abstiennent de cibler les infrastructures critiques d'autres États, mais sans clause limitant précisément les méthodes techniques ou les programmes d'attaque qui pourraient être utilisés contre des infrastructures critiques.

Après ces apparentes percées, le processus des GEG a pourtant commencé à se dévoyer. Confronté à des questions de plus en plus épineuses sur les moyens de faire appliquer les normes volontaires définies deux ans auparavant, le GEG de 2017 n'a pas été en mesure de produire un rapport de consensus. La Russie, de son côté, a entrepris de créer un espace distinct de discussion sur les cybernormes sous la forme d'un nouveau groupe de travail à composition non limitée (GTCNL). L'objectif manifeste de ce GTCNL était de permettre une participation plus conséquente et plus équitable. Pourtant, malgré les prétendus avantages de ce groupe de travail, la pression exercée par la Russie pour qu'un nouveau forum voie le jour au sein de l'ONU était plus probablement une tentative de compliquer et de faire dérailler un processus déjà délicat. De nombreux pays craignaient que ce GTCNL crée des cadres normatifs contradictoires et concurrents qui dilueraient encore les effets des rapports non contraignants des GEG.

Le processus des GEG est limité: le Secrétaire général sélectionne les participants dès le départ et ceux-ci sont réduits à un petit nombre de représentants nationaux

(15 à 25). La composition de chaque GEG est également fixe pendant toute sa durée. Le GTCNL, au contraire, regroupe les 193 États membres, ce qui peut le rendre difficile à gérer. Les participants ne sont pas tenus d'assister à toutes les réunions, mais peuvent apporter leur contribution lorsqu'ils jugent bon de le faire. Le GTCNL est également ouvert aux organisations non gouvernementales (ONG): des groupes de la société civile, des universitaires et des acteurs du secteur privé peuvent demander à y participer et faire part de leurs commentaires tout au long du processus. Des groupes accrédités peuvent assister aux réunions du GTCNL en qualité d'observateurs et participer à des consultations informelles.

La volonté russe de promouvoir la souveraineté des États et la sécurité intérieure est de plus en plus en décalage avec la tendance générale des GEG à soumettre les activités des États dans le cyberespace à des restrictions internationales. Dès le lancement de sa proposition en 1998, la Russie a clairement montré que la sécurité intérieure était pour elle une priorité. Ses déclarations ultérieures mettent l'accent sur la «sécurité de l'information», qui intègre les menaces «politiques et idéologiques» émanant du cyberespace, plutôt que sur la «cybersécurité», qu'elle considère comme plus strictement technique. En pratique, la sécurité de l'information englobe les questions liées à la modération et à la restriction des contenus, ce qui permet aux gouvernements d'intervenir plus explicitement dans l'accès à l'information pour assurer la stabilité nationale. Les processus normatifs de l'ONU utilisent des termes plus vagues tels que la «sécurité des TIC» pour tenter d'éluder la question. Dans ce contexte, les tensions sous-jacentes entre deux modèles de cyberespace, l'un plus ouvert et l'autre qui se prête davantage à l'intervention des gouvernements, continuent de freiner les avancées à New York et à Genève.

Évolutions récentes

Malgré les préoccupations initiales quant à un processus à deux voies au sein de l'ONU, l'année 2021 a été marquée par une réussite surprenante dans le domaine des cybernormes. Le sixième GEG a débouché sur un rapport de consensus qui présente une avancée prudente sur la question du DIH et de son applicabilité potentielle à l'utilisation des TIC par les États. La Suisse a été l'un des principaux défenseurs de l'extension du DIH aux cyberactivités. Elle a ainsi publié, en annexe au rapport du GEG, une prise de position dépassant les conclusions du rapport pour affirmer que le DIH constituait le principal corpus de droit régissant les cyberopérations lors d'un conflit armé. Le premier GTCNL, présidé par l'ambassadeur suisse Jürg Lauber, a également abouti à un rapport de consensus qui appuyait les conclusions des GEG précédents et réaffirmait l'importance des discussions conduites sous la houlette de l'ONU sur les cybertechnologies dans le contexte de la sécurité internationale. L'ambassadeur a également ouvert la voie en sollicitant la participation de petites organisations régionales, élargissant ainsi l'éventail d'expertises présentes au sein du GTCNL. Un deuxième GTCNL a été mis en place en décembre 2021 et prendra fin en 2025.

La Russie et les États-Unis ont aussi pris des mesures pour renforcer leur engagement diplomatique dans le cyberespace. En juin 2021, le président américain Joe Biden et le président russe Vladimir Poutine se sont rencontrés à Genève pour discuter des moyens d'atténuer les tensions et de limiter les cyberattaques contre leurs pays respectifs. Il semble que le nombre de cyberattaques ait quelque peu diminué dans les mois qui ont suivi. Les États-Unis et la Russie ont alors noué une timide relation de travail pour réprimer les pirates malveillants opérant sur leurs territoires. En octobre, la Russie et les États-Unis ont présenté à la Première Commission de l'Assemblée générale des Nations Unies une proposition conjointe soulignant l'engagement des deux pays en faveur des processus du GTCNL et du GEG, ainsi que des rapports de consensus qui en découlent. Cinquante pays ont coparrainé la résolution, qui a été adoptée sans vote au début du mois de novembre.

> Les gouvernements ne sont pas des monolithes dans le cyberespace: la majorité des TIC sont détenues et exploitées par le secteur privé.

Près d'un an plus tard, cette résolution semble être un vestige d'une époque révolue. L'invasion de l'Ukraine par la Russie en février 2022 a entraîné des bouleversements majeurs dans la diplomatie internationale qui ont inévitablement eu des répercussions sur la question des cybernormes. Les relations tendues entre les États-Unis et la Russie ont bloqué toute avancée sur la résolution de novembre et fait monter la température au sein de l'actuel GTCNL. Les cyberactivités ont joué un rôle de soutien essentiel sur les champs de bataille d'Ukraine, notamment lors des premières tentatives russes pour s'emparer de Kyiv et avec l'approche novatrice de l'armée informatique d'Ukraine. Dans les jours qui ont précédé l'invasion de février, la Russie a lancé une attaque sur une chaîne d'approvisionnement qui a perturbé les communications satellite dans tout le pays. Le Kremlin est également à l'origine de diverses attaques collectives par saturation de service et campagnes de destruction de données contre le gouvernement et le peuple ukrainiens. L'armée informatique d'Ukraine, pour sa part, a lancé des campagnes coordonnées visant à défigurer et à surcharger des services web russes, généralement via des attaques collectives par saturation de service. Si l'importance stratégique de ces incidents n'est pas encore claire, l'armée informatique a ouvertement recruté certains de ses membres en dehors de l'Ukraine, notamment dans des États membres de l'UE et de l'OTAN (voir le rapport du CSS: «The IT Army of Ukraine»). Ces évolutions mettent à l'épreuve les conclusions des précédents rapports de consensus et soulèvent des questions majeures autour des obligations de diligence, de la protection des infrastructures critiques et de l'identité des combattants dans le cyberespace.

Le GTCNL en panne

Cependant, l'ONU semble mal outillée pour mieux prendre en compte les réalités du conflit dans son discours normatif. Miné par les querelles de procédure, le GTCNL est également dans l'impasse sur le fond. La participation au groupe de travail a pris un tour particulièrement politique lorsque 32 organisations de la société civile se sont vu refuser l'accès aux sessions de juillet à New York. La Russie est à l'origine de la plupart de ces refus. Bien que le pays n'ait donné aucune explication publique sur ses

Lectures complémentaires

Duncan Hollis, **«A Brief Primer on International Law and Cyberspace»,** *Carnegie Endowment for International Peace* 14.06.2021.

Camino Kavanagh, **«Ukraine: Cyber Operations and Digital Technologies»,** *Directions Blog,* 22.03.2022.

Louise Marie Hurel, **«The Rocky Road to Cyber Norms at the United Nations»,** *Council on Foreign Relations,* 06.09.2022.

décisions, une grande partie des groupes exclus avaient un ancrage occidental. L'Ukraine a également refusé quelques organisations au motif qu'elles étaient trop étroitement liées à l'État russe pour que l'on puisse véritablement les considérer comme des participants non gouvernementaux.

Le rejet des ONG en juin porte atteinte à un atout déterminant du processus du GTCNL: son ouverture. De par sa structure, ce groupe de travail permet à un éventail plus souple et plus inclusif d'acteurs de participer au débat normatif. Les gouvernements ne sont pas des monolithes dans le cyberespace. À travers le monde, la majorité des TIC sont détenues et exploitées par le secteur privé, et les infrastructures critiques échappent de plus en plus aux mains des États. Des organisations de la société civile qui fournissent une expertise et des capacités importantes pour traiter et résoudre les incidents aux multinationales qui gèrent une grande partie d'Internet, les ONG jouent déjà un rôle clé dans la gouvernance de facto du cyberespace. Exclure ces groupes du processus de définition et de mise en œuvre des normes est donc une stratégie à courte vue. En effet, qu'elles participent ou non aux sessions à New York, des organisations comme le Cyber Tech Accord (un consortium représentant les principaux intérêts du secteur privé américain et européen dans le domaine des TIC) et le FIRST (un réseau mondial d'intervenants en cas d'incident informatique) conserveront une place majeure dans le cyberespace.

Les forums multilatéraux de l'ONU restent des pierres de touche importantes pour le débat.

Impasse sur le fond

Comme on pouvait s'y attendre, le GTCNL en a encore moins fait pour résoudre les querelles de fond. Même dans le domaine des mesures de confiance, c'est-à-dire les activités et processus mis en place pour réduire les tensions ou la méfiance entre les États et limiter ainsi le risque d'escalade et de conflit, le GTCNL s'est retrouvé dans l'impasse. Une hotline en cas de cybercrise, rappelant la célèbre ligne téléphonique d'urgence en cas de crise nucléaire établie entre Moscou et Washington pendant la guerre froide, a été proposée lors de réunions précédentes. Or, le GTCNL n'a pas été en mesure de progresser sur un plan de mise en œuvre précis. Une recommandation visant à renforcer la coopération des équipes d'intervention en cas d'urgence informatique a même été retirée du rapport final. Si le GTCNL ne parvient pas à avancer dans des domaines qui paraissent peu sujets à controverse, sur quoi peut-il espérer trouver un terrain d'entente?

Le GTCNL a également buté sur la question du DIH et de son applicabilité au cyberespace. Le DIH est devenu un point de discorde majeur, particulièrement dans le contexte de la guerre russe en Ukraine. Les GEG précédents et l'actuel GTCNL n'ont pas pu aller au-delà d'allusions extrêmement vagues aux fondements du DIH, en indiquant par exemple que les principes de proportionnalité et de distinction pourraient être valables dans le cyberespace. Les rapports de consensus ne contiennent pas non plus un mot au sujet des applications spécifiques. Les cyberopérations trouvent pourtant leur place sur le champ de bataille, et les principes du DIH entrent clairement en jeu. Les questions sur la définition d'un combattant et sur les actions considérées comme proportionnelles et distinctives finiront par se poser dans d'autres pans du droit international. Mais dans le climat actuel, toute avancée sur ces sujets semble aussi urgente qu'improbable.

Perspectives

La stagnation du GTCNL témoigne d'un environnement géopolitique de plus en plus fracturé et marqué par l'intensification des tensions entre la Russie et l'Occident. Malgré ses avancées limitées cette année, de nombreux membres du groupe ont fait valoir que son existence même constituait une mesure de confiance. Les forums multilatéraux de l'ONU restent des pierres de touche importantes pour le débat, d'autant que d'autres voies diplomatiques se sont effondrées depuis un an. À l'évidence, le fait même que la Russie, l'Ukraine, les États-Unis et l'UE se soient réunis en mars et en juillet à New York pour discuter des cybernormes relève du miracle. Pour la Suisse, le maintien d'un discours normatif de la part de l'ONU montre que beaucoup d'États attachent encore de l'importance à ce que le cyberespace reste stable et gouvernable.

S'il y a peu de chances que le processus de l'ONU enregistre des avancées majeures à court et moyen terme, la Suisse a clairement intérêt à ce qu'il demeure crédible et ouvert. La Confédération a soutenu l'inclusion significative des ONG dans le processus de l'ONU et, notamment grâce aux efforts helvétiques de plaidoyer , le GTCNL a ouvert la voie à divers espaces de discussion sur les normes à l'échelle régionale et non gouvernementale. Espérons que ces débats donneront des résultats plus fructueux. En effet, cette profusion de cadres plus restreints constitue un signal bienvenu: tandis que l'Occident et la Russie se trouvent dans une impasse prolongée, d'autres pays tentent de faire un pas en avant.

Voir le site thématique du CSS pour en savoir plus sur les politiques de cybersécurite.

Taylor Grossman est Senior Researcher au sein de l'équipe «Risk and Resilience» du Center for Security Studies (CSS) à l'ETH de Zürich.

Les **analyses de politique de sécurité** du CSS sont publiées par le Center for Security Studies (CSS) de l'ETH de Zürich. Le CSS est un centre de compétence en matière de politique de sécurité suisse et internationale. Deux analyses paraissent chaque mois en allemand, français et anglais.

Éditrice : Névine Schepers
Révision linguistique : Névine Schepers
Layout et graphiques: Miriam Dahinden-Ganzoni

Feedback et commentaires: analysen@sipo.gess.ethz.ch
Plus d'éditions et abonnement: www.css.ethz.ch/cssanalysen

Parus précédemment:

La Russie, puissance nucléaire No 312
Séoul renforce ses ambitions en matière de défense No 311
L'adhésion de la Finlande à l'OTAN No 310
Concept stratégique de l'OTAN: des ambitions modérées No 309
Enjeux géopolitiques de la transition énergétique No 308
La défense française à la croisée des chemins No 307

ISSN: 2296-0228; DOI: 10.3929/ethz-b-000578849